UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/998,319	12/03/2001	Stephen M. Matyas JR.	PPS01-100	5577

7590 04/20/2005

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/998,319	MATYAS ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☒ Claim(s) *1-29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/21/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 12/03/2001.

1. Claims 1-29 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. This application does not claim priority.

4. The effective filing date for the subject matter defined in the pending claims in this application is 12/03/2001.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/21/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on 12/03/2001 are acceptable for examination proceedings.

Specification

7. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

8. The abstract of the disclosure is objected to because

The abstract of the disclosure does not comply with the length requirement as it is more that 150 words.

Correction is required. See MPEP § 608.01(b).

9. The disclosure is objected to because it contains embedded hyperlinks and/or other form of browser-executable code. Applicant is required to delete all embedded hyperlinks and/or other forms of browser-executable code. (See pages 2, and 14 of the specification for examples, but the entire specification should be checked as well.)

See MPEP § 608.01. Appropriate correction is required.

Claim Objections

10. Claims 3-7, and 9-17 are objected to because they contain the abbreviated identifier "PE" but do not specify this definition of this identifier in the claims, which leads to a lack of antecedent basis in the claims.

11. Claim 11 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 11 is the same as its direct parent claim 10.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 1-29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

14. A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. See MPEP § 2173.05(c). Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claim 1, 19, 20, 25, 26, and 27 recite the broad recitation "set of answers", and the claim also recites "and possibly other information" which is the narrower statement of the range/limitation. The ordinary person would be unable to determine if the "other information" was required by the claim or not and therefore would be unable to determine the scope of the claim. Therefore, claims 1-29 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

16. Claims 1-3, 5, 8-9, 18-20, and 23-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Ellison et al. ("Protecting Secret Keys with Personal Entropy") hereinafter referred to as Ellison.

17. Regarding claim 1, Ellison disclosed a method enabling a user of a computing system to generate a secret value from answers to questions previously created by the user (See Ellison Abstract and Page 2 Paragraph 5), said method comprising the steps of displaying the questions previously created by the user (See Ellison Page 5 Line 11 and Section 4 Paragraph 1); prompting the user to select a first portion of the displayed questions and provide a first set of answers to the selected first portion of questions (See Ellison Section 4 Paragraph 1), attempting to generate said secret value from a portion of the first set of answers and possibly other information (See Ellison Page 5 Lines12-19 and Section 4 Paragraph 1); if said secret value cannot be generated from at least a portion of the first set of answers and possibly other information, prompting the user to select a second portion of the displayed questions and provide a second set of answers to the selected second portion of questions (See Ellison Section 4 Paragraph 1); and attempting to generate said secret value from a portion of said first and second sets of answers and possibly other information (See Ellison Paragraph 1).

18. Regarding claim 2, Ellison disclosed that there are n questions previously created by the user (See Ellison Section 4.2), and the user is prompted to select as said first portion at least m questions to answer (See Ellison Section 4 Paragraph 1 and Section 4.1) but, at the user's option, can select k questions to answer (See Ellison Section 4 Paragraph 1), where $0 < m <= k <= n$ and

the set of k questions consists of a first subset of m questions and an optional subset of k_1, questions ($k_1 = k - m$) (See Ellison Section 4 Paragraph 1).

19. Regarding claim 3, Ellison disclosed that there are n questions previously created by the user, and the user is prompted to select as said second portion a third set k_2 of the n-m-k_1 additional unanswered questions, where $0 < k_2 <= n-m-k_1$ and k_2 is a variable value determined by the PE user (See Ellison Section 4 Paragraph 1).

20. Regarding claim 5, Ellison disclosed that the at least one of the values k_1 and k_2 is a constant (See Ellison Section 4 Paragraph 1 and Page 6 Lines 16-20).

21. Regarding claim 8, Ellison disclosed that there are n questions previously created by the user, and the user is prompted to select as said first portion m questions to answer, where $0 < m < n$, and the user is prompted to select as said second portion 1 to n-m as said second portion (See Ellison Section 4 Paragraph 1).

22. Regarding claim 9, Ellison disclosed that there are n questions previously created by the user, and the user is prompted to select as said first portion at least m questions to answer but, at the user's option, can select k questions to answer, where $0 < m <= k <= n$ and the set of k questions consists of a first subset of m questions and an optional subset of k_1 questions ($k_1 = k - m$), (See Ellison Section 4 Paragraph 1) and wherein the PE user is authenticated of m questions and answers in a predetermined way from among the questions and answers specified by the PE user (See Ellison Section 4 Paragraph 1).

23. Regarding claim 18, Ellison disclosed authentication based on generating the secret value and displaying incorrect answers to the user (See Ellison Page 5 Lines 11-19 and page 10 lines 23-33).

24. Regarding claim 19, Ellison disclosed a method enabling a user of a computing system to generate a secret value from answers to questions previously created by the user, said method comprising the steps of: displaying the questions previously created by the user; prompting the user to select a first portion of the displayed questions and provide a first set of answers to the selected first portion of questions; attempting to generate said secret value from a portion of the first set of answers and possibly other information; prompting the user to select a second portion of the displayed questions and provide a second set of answers to the selected second portion of questions; attempting to generate said secret value from a portion of said first and second sets of answers and possibly other information; prompting the user to select a third portion of the displayed questions and provide a third set of answers to the selected third portion of questions, if said secret value cannot be generated from at least a portion of the first and second sets of answers and possibly other information', and attempting to generate said secret value from a portion of said first, second, and third sets of answers and possibly other information, if said secret value cannot be generated from at least a portion of the first set of answers and possibly other information (See Ellison Page 5).

25. Regarding claim 20, Ellison disclosed a method enabling a user of a computing system to generate a secret value from answers to questions previously created by the user, said method comprising the steps of: displaying the questions previously created by the user; prompting the user to select at least a portion of the displayed questions and provide answers to the selected portion of questions; attempting to generate said secret value from a first sub-portion of the provided answers and possibly other information; and if said secret value cannot be generated from said first sub-portion of the provided answers and possibly other information, attempting to

generate said secret value from a second sub-portion of the provided answers (See Ellison Page 5).

26. Regarding claims 22-24, Ellison disclosed that the second subset was chosen randomly from all the questions and therefore could contain none of the first set, some of the first set, or all of the first set (See Ellison Section 4 Paragraph 1).

27. Regarding claim 25, Ellison disclosed a method enabling a user of a computing system to generate a secret value from answers to questions previously created by the user, said method comprising the steps of: displaying the questions previously created by the user; prompting the user to select a first portion of the displayed questions and provide a first set of answers to the selected first portion of questions; prompting the user to select a second portion of the displayed questions and provide a second set of answers to the selected second portion of questions', attempting to generate said secret value from a portion of the first set of answers and possibly other information; and if said secret value cannot be generated from at least a portion of the first set of answers and possibly other information, attempting to generate said secret value from a portion of the first and second sets of answers and possibly other information (See Ellison Page 5).

28. Regarding claim 26, Ellison disclosed that if said secret value cannot be generated from at least a portion of the first and second sets of answers and possibly other information, further comprising the step of prompting the user to select a third portion of the displayed questions and provide a third set of answers to the selected third portion of questions (See Ellison Section 4 Paragraph 1).

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

30. Claims 4, 6-7, and 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison.

31. Regarding claims 4 and 10-11, Ellison disclosed that the PE user is allowed to repeat the step of selecting as said second portion a third set k_2 of the unanswered questions until one of the following conditions is met: (1) the PE user is successfully authenticated, or (3) the PE user fails to be authenticated after answering all n questions (See Ellison Section 4 Paragraph 1 and Page 5 Lines 16-19), but failed to disclose that the user can give up. It would have been obvious to the ordinary person skilled in the art at the time of invention that a user may give up. This would have been obvious because the ordinary person skilled in the art would have realized that it was human nature to give up after a some amount of failed attempts to authenticate oneself.

32. Regarding claims 6, Ellison disclosed that the user was too decide on the number of questions and the number needed to be answered correctly in order to pass the authentication (See Ellison Sections 4.1-4.2 especially Page 7 Lines 5-14 and Table on Page 7), wherein the user would need to experiment to determine the probability of answering a question correctly, and the amount of failures the user is willing to accept. It would have been obvious to the ordinary person skilled in the art at the time of invention that through experimentation, a user is likely to find that the optimum number of total questions for them is 9 and the optimum number

of correct answers for the user to be authenticated is 4. This would have been obvious because the ordinary person skilled in the art would have recognized that a user who is willing to accept more failures than the user in the example given by Ellison would have found an optimization of 9 total questions and 1-4 or more correct answers.

33. Regarding claim 7, it was inherent that if n=9 and m=5 and k_1=0, that when the user tried a second combination of questions as disclosed in Section 4 Paragraph 1 of Ellison, the number of differing questions would have to equal 1, 2, 3, or 4.

34. Claims 12-14 are rejected for the same reasons as claims 5-7 above as applied to claim 11 above.

35. Claims 15-17, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison as applied to claims 1 and 20 above, and further in view of Khan et al. (US Patent Number 6.401.206) hereinafter referred to as Khan. Ellison disclosed requiring a certain number of correct answers to questions in order to authenticate a user (See Ellison Section 4 Paragraph 1) but failed to disclose increasing the number when the user answered too many questions incorrectly in a previous attempt.

Khan teaches that in a question based authentication system that the number of correct answers required to authenticate a person should depend on the level of security desired and further that the level of security should be increased when a user fails the authentication process (See Khan Col. 9 Paragraph 3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Khan in the authentication system of Ellison by increasing the number of correct answers required for authentication in the event that a user failed the prior

attempt to authenticate. This would have been obvious because the ordinary person would have been motivated to further protect against an attempt by an attacker to break the authentication.

36. Claims 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison, and further in view of Intel ("Intel Internet Authentication Services").

37. Regarding claim 27, Ellison disclosed a user being authenticated by being prompted with questions that the user previously created, the user selecting a portion of the answers to the questions to submit for authentication and if the user was not authenticated the user selecting a different portion of the answers to submit for authentication (See Ellison Page 5), but failed to disclose the system being over a network using applets downloaded from one server and authentication steps performed on another server.

Intel teaches that a question based authentication system can be used over a network (See Intel Page 7 Fig. 1) and that in order to make the authentication as convenient as possible, an applet should be transparently downloaded from one server to the user to prompt for user authentication input that will be verified at an authentication server (See Intel Pages 7-9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Intel in the question based authentication service of Ellison by providing authentication across a network using applets. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection to network servers in a user friendly, simple and intuitive manner.

38. Regarding claim 28, the combination of Ellison and Intel disclosed a repository of downloadable client applets attached to the controller computer, the client applets being downloadable to the user client computer and used for both creating the secret value from

answers supplied by the user when originally creating the questions and, later, generating the secret value from answers provided by the user to subsets of the previously created questions (See Intel Page 7 Col. 3 Part 3 and Page 8 Col. 2 Part 9a and Col. 3 Part 9c).

39. Regarding claim 29, the combination of Ellison and Intel disclosed a central database maintained by the authentication server computer, said central database containing information created by users which can be subsequently accessed by the controller server computer on behalf of the user (See Intel Fig. 2 Authentication Databases).

Conclusion

40. Claims 1-29 have been rejected.

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Mark (US Patent Number 5,907,597) disclosed a system for authenticating users using questions previously answered by the user.

b. Chow et al. (US Patent Application Publication 2004/0078775) disclosed an authentication system based on personal questions.

c. Fischer (US Patent Number 6,141,423) disclosed a system for escrowing digital secrets involving secret sharing of shares encrypted with passwords.

d. Chamley et al. (US Patent Number 6,804,786) disclosed a system for authentication involving user generated questions and answers.

e. Endo (US Patent Number 4,528,442) disclosed a system for associating a user with a card based on questions and answers.

42. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
4/15/2005

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER